UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information related to the Dropbox account 519359234 with email p_4_r_4_d_0_x@hotmail.com

Case No. 1:19MJ384

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Information related to the Dropbox account 519359234 with email p_4_r_4_d_0_x@hotmail.com, stored at premises owned, maintained, controlled or operated by Dropbox, Inc. as further described in Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence of, instrumentalities used in committing, and fruits of the crimes of 18 U.S.C. Sections 2252A(a)(2)(A) and 2252A(a)(5)(B) as further described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)(A)	Receipt/Distribution of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

M.C. Glenn Covington
Applicant's signature

M.C. Glenn Covington, HSI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/11/19 11:25am

Joi Elizabeth Peake
Judge's signature

City and state: Winston Salem, North Carolina

Joi Elizabeth Peake, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent M.C. Glenn Covington with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI), currently assigned to Cary, North Carolina, being first duly sworn, hereby make the following statement in support of an application for a search warrant:

INTRODUCTION

1. I make this affidavit in support of an application for a warrant to search information related to Dropbox accounts 519359234 and 193876494 with email addresses p_4_r_4_d_0_x@hotmail.com paradoxincorporated@gmail.com, respectively (hereafter "SUBJECT ACCOUNTS"). The information is stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., a company headquartered at 185 Berry Street, San Francisco, California 94107. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(l)(A) and 2703(c)(l)(A) to require Dropbox, Inc. to disclose to the government records and other information in its possession, pertaining to the SUBJECT ACCOUNTS.

2. I am investigating Philip Stephen STALLINGS (hereafter STALLINGS) for distribution, receipt, and possession of child pornography and I have probable cause to believe that contraband and evidence of a crime, fruits

of a crime, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B) are located within the SUBJECT ACCOUNT.

3. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located within the SUBJECT ACCOUNTS.

AFFIANT BACKGROUND

4. I am a Special Agent with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI), currently assigned to Cary, North Carolina and have been so employed since October 2009. I am responsible for investigations involving the production, importation, advertising, receipt, and distribution of child pornography which occur in the Middle District of North Carolina. I was previously employed as a United States Postal Inspector for five years in Richmond, VA and was responsible for child exploitation investigations involving the U.S. Mail. I have participated

in over 400 child pornography investigations. I have received training in the area of child pornography and child sexual exploitation as well as specialized instruction on how to conduct investigations of child sexual exploitation and child pornography crimes through the United States Postal Inspection Service, the FBI and the Department of Justice. I have also received specialized training from the Internet Crimes Against Children Task Force seminars and at the Dallas, Texas Advocacy Center's Crimes Against Children Training Conference.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns violations of the following statutes:

a. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).

b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has

been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(2).

DROPBOX

6. Dropbox Inc. is a file hosting and sharing service operated by Dropbox Inc., which is headquartered in San Francisco, California and is an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computer service, as defined in 18 U.S.C. § 2711(2). Dropbox.com offers to its users cloud storage, file synchronization, personal cloud, and client software. Online storage mediums, such as Dropbox, make it possible for a user to access saved files without the requirement of storing said files on their own computer or other device. A Dropbox user can store digital files within a special folder on the user's device, and these files can be synchronized so the same folder with all the same digital content is accessible on each of the user's other devices which have the Dropbox application installed and synched with the user's account. Files placed in these folders may be accessed through the Dropbox website and through desktop and mobile device applications.

7. Dropbox users can share access to their digital files with others by using the built in option to create URL hyperlinks to their Dropbox accounts ("links") and sending said links through email or social media accounts. Dropbox users can also allow others to upload and download digital files stored within specific shared folders in the user's account. Dropbox has desktop applications as well as mobile applications for Android, and iOS devices. Dropbox collects information like the user's name, email address, phone numbers, payment info, and physical address. Dropbox also collects IP addresses for the devices accessing the account, the type of browser, device used, as well as identifiers associated with the user's devices.

8. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

BACKGROUND ON KIK AND KIK REPORTS

9. Kik Messenger (hereinafter "Kik") is a mobile application designed for chatting or messaging that was, until recently, owned and operated by Kik

Interactive, Inc.[1] According to the document "Kik's Guide for Law Enforcement," to use this application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

10. According to "Kik's Guide for Law Enforcement," Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text messages, images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.

[1] In October 2019, United States based company, MediaLab, acquired the KiK Messenger application.

11. According to information provided to HSI by a Kik Law Enforcement Response Team Lead, Kik's Terms of Service prohibit Kik users from uploading, posting, sending, commenting on, or storing content that contains child pornography and/or child abuse images. The Terms of Service also provide that Kik may review, screen and delete user content at any time if Kik believes use of their services are in violation of the law. According to Kik, Kik has a strong business interest in enforcing their Terms of Service and ensuring that their services are free of illegal content, and in particular, child sexual abuse material. Accordingly, Kik reports that it independently and voluntarily takes steps to monitor and safeguard their platform and that ridding Kik products and services of child abuse images is critically important to protecting their users, product, brand, and business interests.

12. Kik Interactive, Inc. is located in Ontario, Canada and is governed by Canadian law. According to information contained in the "Kik Interactive, Inc. Child Sexual Abuse and Illegal Material Report and Glossary" (hereinafter Kik Glossary), which Kik Interactive, Inc. provided when reporting information to law enforcement authorities, Kik Interactive, Inc. was mandated to report to the Royal Canadian Mounted Police (RCMP) any images and/or videos that would constitute suspected child pornography under Canadian law which were discovered on the Kik platform. According to the Kik Glossary, Kik was typically alerted to suspected child pornography on Kik

based on digital hash value matches to previously identified child pornography or through reports from other Kik users or third party moderators.

13. According to the Kik Glossary, Kik enables users to report other users who have abused or harassed them within the application, using an in-application reporting feature. When a Kik user reports another user, they have the option to include their full conversation history, including text, and any images or videos sent between them. Kik refers to this type of report as an "Abuse Report."

14. According to the Kik Glossary, Kik uses PhotoDNA to automatically scan user-uploaded files in order to flag content that may depict suspected child pornography and prevent such images from continuing to circulate through their application. When PhotoDNA detects a suspected child pornography file, it creates a Report and sends it to the Kik Law Enforcement team. Kik refers to this type of report as a "PhotoDNA Report."

15. According to information provided by a Kik Law Enforcement Response Team Lead, all suspected child pornography images and videos reported via a PhotoDNA Report or an Abuse Report, as well as any related user communications, are visually reviewed by a member of the Kik Law Enforcement Response team before a report is forwarded to law enforcement authorities. Kik trains employees comprising its Law Enforcement Response team on the legal obligation to report apparent child pornography. The Team

is trained on the Canadian statutory definition of child pornography and how to recognize it on Kik products and services. Kik voluntarily makes reports to law enforcement in accordance with that training. After Kik discovers suspected child pornography, Kik removes the content from its communications system and closes the user's account.

16. The RCMP has advised Homeland Security Investigations (HSI) agents that upon receiving a report from Kik related to suspected child pornography, the RCMP reviewed the reported IP addresses of the Kik users contained in the Kik Reports to determine their location. The RCMP then provided Kik Reports of Kik users in the United States to HSI in Ottawa, Canada, who in turn provided the Kik Reports to the HSI Cyber Crimes Center (C3) Child Exploitation Investigations Unit (CEIU) located in Fairfax, Virginia for analysis and dissemination.

BACKGROUND OF THE INVESTIGATION

17. In December 2018, HSI received three Kik reports for three separate Kik users, "paradox.inc", ".mrparadox.", and "_mrparadox_". The reports concerned the same IP address and the same image of child pornography.

Kik Report for Username "paradox.inc":

18. On December 3, 2018, HSI received a Kik Report concerning user

"paradox.inc". The report revealed that, on November 30, 2018 at 12:59 PM EST, paradox.inc used IP address 107.15.247.146 to upload a child pornography image to Kik's servers. Kik was alerted to the image by a PhotoDNA Report. I have reviewed the image and it depicts the following:

> Two minor females ages 7 to 11 years old squatting on a table with their arms behind them and legs spread apart exposing their genitals in sexually explicit manner. On the right corner of the image appears the phrase "LS-Magazine".

19. Subscriber records for paradox.inc provided by Kik reveal a "registration timestamp" of November 26, 2018 at 10:30 EST. The user listed his first name as "Paradox" and his last name as "Inc". The user provided an email of "fuckoff4@fuckoff4.com" and a date of birth May 1, 1980. The Kik records list the email as unconfirmed.[2] The user's device is identified as a Samsung Galaxy J3 Emerge (model number: SM-J327P).

20. A Kik IP address log reveals that Kik user paradox.inc used IP address 107.15.247.146 fifty-nine times between November 26, 2018 and November 30, 2018. Further, it is the only IP address listed in the log.

Kik Report for Username ".mrparadox.":

21. On December 24, 2018, HSI received a Kik Report concerning user

---

[2] "Unconfirmed" means either that the email address is either invalid, or the user received a confirmation email from Kik but didn't click on the link to confirm.

".mrparadox.". The report reveals that, on December 22, 2018 at 1:37 AM EST, .mrparadox. used IP address 107.15.247.146 to send a child pornography image to another user(s) via a Kik chat. Kik was alerted to the image by a Kik user who lodged an Abuse Report. I have reviewed the image and it depicts the following:

> Two minor females ages 7 to 11 years old squatting on a table with their arms behind them and legs spread apart exposing their genitals in sexually explicit manner. On the right corner of the image appears the phrase "LS-Magazine".

22. Subscriber records for .mrparadox. provided by Kik reveal a "registration timestamp" of December 19, 2018 at 10:12 AM EST. The user listed his first name as "Paradox" and his last name as "Inc". The user provided an email of "fuckoff12fuckoff12.com" and a date of birth May 1, 1980. The Kik records list the email as unconfirmed. The user's device is identified as a Samsung Galaxy J3 Emerge (model number: SM-J327P).

23. A Kik IP address log reveals that Kik user .mrparadox. used IP address 107.15.247.146 numerous times between December 19, 2018 and December 22, 2018. Further, it is the only IP address listed in the log.

Kik Report for Username " mrparadox ":

24. On December 24, 2018, HSI received a Kik Report concerning user "_mrparadox_". The report reveals that, on December 22, 2018 at 2:31 AM EST, _mrparadox_ used IP address 107.15.247.146 to send a child pornography

image to another user(s) via a Kik chat. Kik was alerted to the image by a Kik user who lodged an Abuse Report. I have reviewed the image and it depicts the following:

> Two minor females ages 7 to 11 years old squatting on a table with their arms behind them and legs spread apart exposing their genitals in sexually explicit manner. On the right corner of the image appears the phrase "LS-Magazine".

25. Subscriber records for _mrparadox_ provided by Kik reveal a "registration timestamp" of December 22, 2018 at 2:26 AM EST. The user listed his first name as "Paradox" and his last name as "Inc". The user provided an email of "fuckoff13fuckoff13.com" and a date of birth May 1, 1980. The Kik records list the email as unconfirmed. The user's device is identified as a Samsung Galaxy J3 Emerge (model number: SM-J327P).

26. A Kik IP address log reveals one entry for _mrparadox_, IP address 107.15.247.146 on December 22, 2018 at 2:26 AM EST.

Identification of Durham Residence:

27. A query of the American Registry for Internet Numbers ("ARIN") online database revealed IP address 107.15.247.146 as being registered to Charter Communications Inc.

28. An administrative summons was issued to Charter Communications, Inc. for account subscriber information for the individual assigned IP address 107.15.247.146. As a result of the summons, Charter

Communications, Inc. provided the following account information;

Subscriber Name:	Philip STALLINGS
Subscriber Address:	2691 Hitchcock Dr. Durham, NC 27705
Phone Number:	(919) 685-5567

The Charter Communications, Inc. records indicate that IP address 107.15.247.146 was assigned to the account of Philip STALLINGS account from at least June 8, 2018 to January 4, 2019.

29. A search of a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for Philip STALLINGS. These public records indicated that Philip STALLINGS's current address was 2691 Hitchcock Dr., Durham, North Carolina 27705 (the SUBJECT PREMISES) and his date of birth is December 29, 1978. On or about April 26, 2019, representatives of the U.S. Postal Service informed me that Philip STALLINGS was receiving mail at the SUBJECT PREMISES. On June 4, 2019, I rang the doorbell at the SUBJECT PREMISES and Philip Stephen STALLINGS answered the door and I asked if he was "Tom Covington." STALLINGS answered no and I left.

30. On June 18, 2019, in the Middle District of North Carolina, Magistrate Judge L. Patrick Auld issued a warrant (1:19mj205) authorizing the search of the SUBJECT PREMISES.

31. On June 18, 2019, I conducted an open source check on Google for

"Philip Stallings, Durham, NC" and located a link for "Images for Philip Stallings, Durham, NC". I clicked the link and observed a screenshot of a Facebook page purportedly belonging to "Philip STALLINGS" with a photograph (profile picture) of STALLINGS on the bottom left hand corner of the screenshot. In parentheses under STALLINGS's name is the name "Mr-Paradox".

32. On June 19, 2019 at approximately 6:18 AM, I and other law enforcement officers executed the search warrant at the SUBJECT PREMISES. Entry was made into the residence and no one was at home. There was one bedroom in the residence. Agents located several computers, hard drives, and thumb drives. It appeared that Philip STALLINGS resided at the residence by himself; though a few articles of female clothing were located in the closet. STALLINGS's identification card was in a wallet that was located on the kitchen counter.

33. Durham County Sheriff's Office (DCSO) deputies located Stallings at Coffee World, 3799 Guess Road, Durham, North Carolina 27705. STALLINGS was arrested pursuant to a 2017 unserved state warrant for Cyberstalking issued in Durham County. Search incident to arrest, a silver Samsung cell phone was recovered from Philip STALLINGS's person.

34. A forensic preview was conducted on a Hewlett Packard laptop computer that was found in the bedroom of the SUBJECT PREMISES. The

preview revealed hundreds of images/videos of minor females lasciviously displaying their genitalia. I recognized some of the content to be consistent with "LS Models" child pornography series which I have encountered in previous investigations. Also observed on the laptop during the preview was a Paltalk user account name of "Mr.Paradox" and a Skype ID of "mister.paradox". A subsequent more thorough forensic examination of the laptop revealed that it contained over 2000 files depicting child pornography. These files included adults engaging in sexual acts with minors

35. STALLINGS's silver Samsung cell phone was forensically examined. The examination revealed four images depicting child pornography located at the following file path: Media/Phone/Android/data/com.dropbox.andriod/files/u193876494/scratch/K-Grade. The files are described below:

> A color image of a 5 to 8-year-old naked female sitting on the bed with her legs spread apart exposing her genitals.
>
> A color image of an infant/toddler female with her genitals exposed and an adult finger is inserted into the infant/toddlers anus.
>
> A color image of a 3 to 5-year-old female laying on an adult male. The male's penis is touching the female's genitals.
>
> A color video of an adult male inserting his penis into a 4 to 6 year old female's anus.

36. The forensic examination of the silver Samsung cell phone also revealed one video depicting child pornography located at the following file path:

Media/Phone/Android/data/com.dropbox.android/files/u193876494/scratch/Movies. The file is described below:

> A color video of an adult male inserting his penis into a 4 to 6-year-old female's anus.

37. Based on my training and experience, as well as conversations with other law enforcement officers that investigate child exploitation cases, I know that individuals who use Kik Messenger to traffic in child pornography often store child pornography in Dropbox accounts and share child pornography on Kik Messenger via Dropbox hyperlinks. In fact, this has become one of the more common means of storing and disseminating child pornography.

38. Dropbox records reveal that the Dropbox account with User ID 193876494 is registered to "Paradox Incorporated" with a listed email address of paradoxincorporated@gmail.com. Further, the IP address 107.15.247.146 was used by the account in June and October 2018. During the forensic examination of STALLINGS's HP laptop, several email addresses, including paradoxincorporated@gmail.com, were found to have been associated with the device. Specifically, the email addresses were autofill artifacts from the Opera

web browser. This means that the email addresses were, at least once, input into a field within the Opera web browser and recorded by the autofill function of the web browser.

39. There is probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located within Dropbox account 193876494 with listed email address paradoxincorporated@gmail.com. The probable cause is based upon the fact that child pornography was located on three of STALLINGS's devices, the child pornography located on his phone was within the file structure for Dropbox account with User ID 193876494 as described in paragraphs 35 and 36, and STALLINGS used multiple Kik Messenger accounts to send and/or receive child pornography and I know that individuals who use Kik Messenger to interact with child pornography often store child pornography using Dropbox.

40. A forensic examination was conducted on a loose WD internal hard drive recovered from the SUBJECT PREMISES. The examination revealed over 1500 files depicting child pornography. These files included both depictions of minors lasciviously displaying their genitalia and adults engaging in sexual acts with minors. During the forensic examination of the hard drive, several email addresses, including p_4_r_4_d_0_x@hotmail.com, were found to have been associated with the device. Specifically, the email addresses were

autofill artifacts from the Opera web browser. This means that the email addresses were, at least once, input into a field within the Opera web browser and recorded by the autofill function of the web browser.

41. Dropbox records reveal that the Dropbox account with User ID 519359234 is registered to "DJ Paradox" with a listed email address of p_4_r_4_d_0_x@hotmail.com. Further, the IP address 107.15.247.146 was used by the account in July 2018.

42. There is probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located within Dropbox account 519359234 associated with listed email address p_4_r_4_d_0_x@hotmail.com. The probable cause is based upon the fact that child pornography was located on three of STALLINGS's devices, child pornography located on STALLING's phone was within the file structure for a different Dropbox account as described in paragraphs 35 and 36, and STALLINGS used multiple Kik Messenger accounts to send and/or receive child pornography and I know that individuals who use Kik Messenger to interact with child pornography often store child pornography using Dropbox.

INFORMATION REGARDING INFORMATION TO BE SEIZED

43. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A)

and 2703(c)(1)(A), by using the warrant to require Dropbox Inc., to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment A. Upon receipt of the information described in Section I of Attachment A, government-authorized persons will review that information to locate the items described in Section II of Attachment A.

44. Because the warrant will be served on Dropbox Inc., who will then compile the requested records at a time convenient to Dropbox Inc., reasonable cause exists to support execution of the requested warrant at any time day or night.

CONCLUSION

45. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States ... that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

M.C. Glenn Covington
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 11 day of December, 2019.

Joi Elizabeth Peake
United States Magistrate Judge
Middle District of North Carolina

ATTACHMENT A

Property to Be Searched

This warrant applies to records and other information related to the Dropbox account 519359234 with email p_4_r_4_d_0_x@hotmail.com, which is stored at any premises owned, maintained, controlled, or operated by Dropbox, Inc., a company headquartered at 185 Berry Street, San Francisco, California 94107.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by Dropbox Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox Inc., including any information that has been deleted but is still available to Dropbox Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox Inc. is required to disclose the following information to the government for each account listed in Attachment A:

a. All files stored and presently contained in, or on behalf of, the account;

b. All transactional information of all activity of the account , including log files revealing the upload, access, and deletion of files, creation or elimination of folder structure, logs reflecting information regarding access to the account, and IP address logs (e.g. IP address, port, date, time, and time zone);

c. All information of any and all activity for any hyperlinks or other access shared by the account, to include the file path of the contents, the creation date of the hyperlink, the hyperlink expiration date, the content made accessible via the hyperlink, all user settings established for the hyperlink, information revealing identifiers (e.g. IP address) of the individuals who accessed the hyperlinks and time of access.

d. All business records and subscriber information, in any form kept, pertaining to the individual account, including subscribers' registration details, full names, addresses, billing addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the device(s) associated with the account, Social Security number, date of birth, telephone numbers, purchase history, email and password records, and other identifiers or records associated with the account;

e. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number.

f. Any and all communications between Dropbox, Inc. and the subscribers of the account.

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 2252A(a)(5)(B) and (a)(2)(A) by the user(s) of the account identified on Attachment A, in the form of the following:

a) records and information constituting child pornography, as defined in 18 U.S.C. 2256(8);

b) records and information constituting child erotica;

c) records and information revealing access to and/or trafficking of child pornography and identity of those participating, to include information about specific transactions and instances of access.

d) records and information revealing the sexual exploitation of or sexual interest in any minor;

e) records and information constituting or revealing the identity and age of any minor victim;

f) transactional and location information pertaining to any items authorized to be seized under this section (Section II), including log files revealing the upload, access, and deletion of files, creation or elimination of folder structure, and information reflecting access;

g) records and information constituting or revealing participation in groups or communication with others that provide or make accessible child pornography; and

h) Records revealing or indicating who created and accessed the Dropbox account identified in Attachment A, including records revealing subscriber information, IP addresses, mobile devices used, and methods of payment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data).

Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, Dropbox, Inc. shall disclose the responsive data by sending it to the below listed contact.

Special Agent M. C. Glenn Covington

Homeland Security Investigations

40 Centrewest Court

Cary, NC 27513

Office: 919 673-8604

Email: marycatherine.g.covington@ice.dhs.gov